

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO**

THERESA MADDEN, an individual,)
on behalf of herself and all others)
similarly situated,)
)
Plaintiff,)
) Civil Action
v.)
) File No. _____
LAKELAND COMMUNITY)
COLLEGE) **JURY TRIAL DEMANDED**
)
Defendant.)

CLASS ACTION COMPLAINT

Plaintiff Theresa Madden, on behalf of herself and all persons similarly situated, alleges:

NATURE OF THE CASE

1. This is a consumer class action lawsuit brought by Plaintiff, individually and on behalf of all others similarly situated (i.e., the Class Members), who entrusted Lakeland Community College (“Lakeland” or “Defendant”) to safeguard their personally identifiable information (“PII”), which includes without limitation name, Social Security number, driver’s license number or state identification number.

2. Lakeland has failed to comply with industry standards to protect information in its systems that contain PII, and has failed to provide timely, accurate, and adequate notice to Plaintiff and other Class Members that their PII had been compromised. Plaintiff seeks, among other things, orders requiring Lakeland to fully and accurately disclose the nature of the information that has been compromised and to adopt reasonably sufficient security practices and safeguards to prevent incidents like this in the future.

3. Lakeland experienced a data security incident between March 7, 2023 and March

31, 2023 that involved Plaintiff's and other consumers' PII (the "Data Breach"). As a result, an unauthorized party accessed certain files and folders within the Defendant's systems and may have viewed, acquired, and/or exfiltrated data containing affected parties' PII. The security incident was wide-reaching, effecting a number of the Defendant's computer systems and compromising the PII of more than 285,000 people.

4. As a result of Defendant's failure to implement and follow basic security procedures, Plaintiff's and Class Members' PII is now in the hands of criminals. Plaintiff and Class Members now and will forever face a substantial increased risk of identity theft. Consequently, Plaintiff and Class Members have had to spend, and will continue to spend, significant time and money in the future to protect themselves due to the Defendant's failures.

5. Accordingly, Plaintiff, individually and on behalf of all others similarly situated, alleges claims for breach of implied contract, unjust enrichment, and injunctive/declaratory relief.

PARTIES

6. Plaintiff Theresa Madden (nee Wayts) lives in Willowick, Ohio and is a citizen of the State of Ohio. Plaintiff is currently a student at Lakeland and has an active account with Lakeland. She first took classes at Lakeland in high school in 2017 and restarted at Lakeland in 2022. She anticipates graduating from Lakeland with a nursing degree in May of 2024. Her PII was collected and maintained by Lakeland and disclosed without authorization to an unknown and unauthorized third party as a result of the Data Breach. *See Exhibit 1* attached hereto for a copy of the Notice Letter that Plaintiff received regarding the Data Breach.

7. Lakeland, based in Kirtland, Ohio, is a community college that serves (and has served) hundreds of thousands of students in their educational pursuits. Founded in 1967,

Lakeland offers various degree programs designed to prepare students to enter the workforce. Lakeland has served hundreds of thousands of students in their educational pursuits and currently employs 924 people and generates approximately \$17.8 million in annual revenue. Its principal place of business is located at 7700 Clocktower Drive, Kirtland, Ohio, 44094 in Lake County. Due to the nature of the services it provides, Lakeland regularly acquires and electronically stores PII belonging to students, prospective students, employees, and other consumers as part of the regular course of its business.

JURISDICTION AND VENUE

8. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive of interest and costs. Upon information and belief, the number of Class Members is over 100, many of whom have different citizenship from Lakeland. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

9. This Court has jurisdiction over Lakeland because Lakeland operates in and/or is incorporated in this District.

10. Venue is proper in this Court pursuant to 28 U.S.C. § 1331(a)(1) because a substantial part of the events giving rise to this action occurred in this District and Lakeland has harmed Class Members residing in this District.

BACKGROUND AND FACTS

11. Lakeland requires that its students and employees entrust it with highly sensitive personal information. Thus, in the ordinary course of receiving employment and educational services from Lakeland, Plaintiffs and Class Members were required to provide their PII to Defendant.

12. In its Privacy Assurance, Lakeland promises its students and employees that it would “protect the quality and integrity of your personally identifiable information.” *See* <https://www.lakelandcc.edu/web/about/privacy-assurance> (last visited 10/12/2023). Lakeland informs all who entrust their PII to Lakeland that Lakeland is “committed to ethical business practices and compliance with all applicable laws, regulations, and policies that govern the privacy of Covered Data.” *See* <https://www.lakelandcc.edu/web/public-policies-and-procedures/policies/3354-2-11-04> (last visited 10/1/2023).

13. Because of the highly sensitive and personal nature of the information Lakeland acquires and stores with respect to its students and employees, Lakeland also promises to, among other things, keep its students’ and employees’ PII private; comply with industry standards related to data security and the maintenance of its students’ and employees’ PII; inform its students and employees of its legal duties relating to data security and comply with all federal and state laws protecting students’ and employees’ PII; only use and release students’ and employees’ PII for reasons that relate to the services it provides; and provide adequate notice to students and employees if their PII is disclosed without authorization.

14. By obtaining, collecting, using, and deriving a benefit from Plaintiffs’ and Class Members’ PII, Lakeland assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs’ and Class Members’ PII from unauthorized disclosure and exfiltration.

15. Plaintiffs and Class Members relied on Lakeland to keep their PII confidential and securely maintained and to only make authorized disclosures of this information, which Defendant ultimately failed to do.

16. In September of 2023, Defendant publicly disclosed that it had “discovered unauthorized access to our network.” *See Ex. 1.*

17. Through the Data Breach, the unauthorized cybercriminal(s) accessed a cache of highly sensitive PII, including full names in connection with Social Security numbers.

18. The Notification Letters were deficient, failing to provide basic details concerning the Data Breach, including, but not limited to, when Defendant first discovered the Data Breach, why sensitive information was stored on systems without adequate security, the deficiencies in the security systems that permitted unauthorized access, whether the stolen data was encrypted or otherwise protected, and whether Defendant knows if the data has not been further disseminated.

19. Lakeland downplayed the seriousness of the incident by failing to take steps necessary to inform Plaintiff and Class Members that their data was in fact stolen by third party bad actors, and that Lakeland, seemingly more out of an abundance of caution, wanted to make Plaintiff and Class Members aware of the Data Breach.

20. Lakeland acknowledges that it is responsible to safeguard Plaintiff and Class Members’ PII. It pledges that it takes privacy very seriously and makes numerous promises that it will maintain the security and privacy of PII.

21. The students and former students of Lakeland entrusted their PII to Lakeland with the mutual understanding that this highly sensitive private information was confidential and would be properly safeguarded from misuse and theft.

22. In addition, as an employer that provides educational services to students and benefits to employees, Lakeland collects and stores highly sensitive medical and private health information (“PHI”) about individuals on its computer systems.

23. The privacy policy posted on Lakeland’s website states: “Your information will be held with the utmost care and will not be used for anything other than official business.”¹

24. Lakeland’s data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

25. Lakeland knew or should have known that its electronic records would be targeted by cybercriminals.

26. Lakeland was well aware that the PII it collects is highly sensitive and of significant value to those who would use it for wrongful purposes. As the Federal Trade Commission (FTC) recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and fraud.² Indeed, a robust “cyber black market” exists in which criminals openly post stolen PII on multiple underground Internet websites, commonly referred to as the dark web.

27. The ramifications of Defendant’s failure to keep PII secure are long lasting and severe. Once stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

28. Further, criminals often trade stolen PII on the “cyber black-market” for years following a breach. Cybercriminals can post stolen PII on the internet, thereby making such information publicly available.

29. The Social Security Administration has warned that identity thieves can use an individual’s Social Security number to apply for additional credit lines. Such fraud may go

¹ See <https://www.Lakeland.edu/privacy-policy/> (last visited June 2, 2023).

² Federal Trade Commission, *Warning Signs of Identity Theft*, available at: <https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft> (last visited June 2, 2023).

undetected until debt collection calls commence months, or even years, later.³ This time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used, compounds an identity theft victim's ability to detect and address the harm.

30. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

31. Further, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security Number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

32. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."⁴

33. Defendant knew, or should have known, the importance of safeguarding PII entrusted to it and of the foreseeable consequences if its systems were breached. This includes

³ *Identity Theft and Your Social Security Number*, Social Security Administrative, available at <https://www.ssa.gov/pubs/EN-05-10064.pdf>.

⁴ Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), available at <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft>.

the significant costs that would be imposed on individuals as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

34. Plaintiff and Class Members now face years of constant surveillance of their records. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

35. Despite all of the publicly available knowledge of the continued compromises of PII, Lakeland's approach to maintaining the privacy of the PII was deficient.

36. In all contexts, time has constantly been recognized as compensable, and for many people, it is the basis on which they are compensated. Plaintiff and Class Members should be spared having to deal with the consequences of Defendant's misfeasance.

37. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.

38. The delay in identifying and reporting the Data Breach caused additional harm to Plaintiff and Class Members. Plaintiff was not timely notified of the Data Breach, depriving her and the Class of the ability to promptly mitigate potential adverse resulting consequences.

39. As a result of Lakeland's failure to prevent the Data Breach, Plaintiff and Class Members have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at increased risk of suffering:

- a. Actual identity theft;
- b. Unauthorized use and misuse of their PII;
- c. The loss of the opportunity to control how their PII is used;
- d. The diminution in value of their PII;

- e. The compromise, publication, and/or theft of their PII;
- f. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;
- g. Lost opportunity costs and lost wages associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;
- h. Costs associated with placing freezes on credit reports;
- i. Delay in receipt of tax refund monies or lost opportunity and benefits of electronically filing of income tax returns;
- j. The imminent and certain impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;
- k. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as it fails to undertake appropriate measures to protect the PII in its possession; and
- l. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

40. To date, Lakeland has not yet disclosed full details of the Data Breach. Without such disclosure, questions remain as to the full extent of the Data Breach, the actual data accessed and compromised, and what measures, if any, it has taken to secure the PII still in its possession. Through this litigation, Plaintiff seeks to determine the scope of the Data Breach and the information involved, obtain relief that redresses any harms, and ensure Lakeland has proper measures in place to prevent another breach from occurring in the future.

41. Lakeland was expressly prohibited by the Federal Trade Commission Act (“FTC Act”) (15 U.S.C. §45) from engaging in “unfair or deceptive acts or practices in or affecting commerce.” The FTC has concluded that a company’s failure to maintain reasonable and appropriate data security for consumers’ sensitive personal information is an “unfair practice” in

violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

42. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.⁵

43. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.⁶ The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

44. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

45. Lakeland failed to properly implement basic data security practices. Its failure to employ reasonable and appropriate measures to protect against unauthorized access to PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

46. Lakeland was at all times fully aware of its obligation to protect PII and was also

⁵ Federal Trade Commission, *Start With Security: A Guide for Business*, available at: <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>.

⁶ Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at: https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

aware of the significant repercussions that would result from its failure to do so.

47. In addition, Lakeland failed to comply with industry standards.

48. Some industry best practices that should be implemented by businesses like Lakeland include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

49. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

50. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

51. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

Plaintiff's Experience

52. When Plaintiff Madden first became a student at Lakeland, they required that she provide substantial amounts of PII as part of the enrollment process. That requirement has continued throughout her relationship with Lakeland.

53. At the time of the Data Breach, Defendant retained Plaintiff's PII in its system. IN addition to her Social Security number and driver's license number, upon information and belief, Lakeland also maintains her name, address, personal mobile number and email address, as well as current payment card information.

54. Plaintiff is very careful about sharing and protecting her PII. Plaintiff stores any documents containing his PII in a safe and secure location. She has never been part of a data breach before and would have never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff would not have entrusted her PII to Defendant had she known of Defendant's lax data security policies.

55. Plaintiff received the Notice Letter, by U.S. mail, from Defendant. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties.

56. As a result of the Data Breach, and the direction of Defendant's Notice Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach. Among other things, she has checked and reviewed her credit information on Credit Karma and she placed a fraud alert with both Transunion and Equifax to ensure her identity is secure. She is also considering changing passwords and resecuring her own computer network and notifying her financial institutions that her accounts have been compromised for any indication of fraudulent activity, which may take years to detect. Plaintiff has spent significant time dealing with the Data

Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

57. Plaintiff suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) lost or diminished value of PII; (ii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iii) invasion of privacy; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

58. Plaintiff further suffered actual injury. She has experienced a noticeable increase in spam telephone calls as well as an increase in the number of spam texts and emails, which, upon information and belief, was caused by the Data Breach and began following the Data Breach.

59. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence.

60. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

61. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

62. Plaintiff has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and

safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

63. Plaintiff brings this action on behalf of herself and all others similarly situated (the “Class”). Plaintiff proposes the following Class definition, subject to amendment as appropriate:

All individuals whose PII was maintained by Lakeland and who were sent a notice of the 2023 Data Breach.

Plaintiff Madden also brings her claims on behalf of a Subclass of Ohio victims with subclass to be defined as follows:

All Ohio individuals whose PII was maintained by Lakeland and who were sent a notice of the 2023 Data Breach.

64. Excluded from the Class are Defendant, Defendant’s subsidiaries and affiliates, its officers, directors, and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representatives, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

65. Plaintiff reserves the right to modify or amend the definition of the proposed Class and Subclass and/or to add classes or subclasses, if necessary, before this Court determines whether certification is appropriate.

66. Numerosity: The Class Members are so numerous that joinder of all Members is impractical. The Class is comprised of over 285,000 individuals. Defendant has the administrative capability through its computer systems and other records to identify all members of the Class and Subclass, and such specific information is not otherwise available to Plaintiff.

67. Commonality: The questions here are ones of common or general interest such that there is a well-defined community of interest among the Members of the Class and Subclass. These questions predominate over questions that may affect only individual class members because Lakeland has acted on grounds generally applicable to the Class and Subclass. Such common legal or factual questions include, but are not limited to:

- a. Whether and to what extent Defendant had a duty to protect the PII of Class Members;
- b. Whether Defendant had duties not to disclose the PII of Class Members to unauthorized third parties;
- c. Whether Defendant took reasonable steps and measures to safeguard Plaintiff's and Class Members' PII;
- d. Whether Defendant failed to adequately safeguard the PII of Class Members;
- e. Whether Defendant breached its duties to exercise reasonable care in handling Plaintiff's and Class Members' PII;
- f. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- g. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;
- h. Whether Plaintiff and Class Members are entitled to actual, damages, statutory damages as a result of Defendant's wrongful conduct;
- m. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct;
- n. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach; and
- o. Whether Plaintiff and Class Members are entitled to additional identity theft protection.

68. Typicality: Plaintiff's claims are typical of the claims of the other members of the Class because Plaintiffs' PII, like that of every other Class Member, was not properly maintained

or secured by Defendant. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Members of the Class were injured through the common misconduct of Lakeland. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

69. It is impracticable to bring the individual claims of the members of the Class and Subclass before the Court. Class treatment permits a large number of similarly situated persons or entities to prosecute their common claims in a single forum simultaneously, efficiently and without the unnecessary duplication of evidence, effort, expense, or the possibility of inconsistent or contradictory judgments that numerous individual actions would engender. The benefits of the class mechanism, including providing injured persons or entities with a method for obtaining redress on claims that might not be practicable to pursue individually, substantially outweigh any difficulties that may arise in the management of this class action.

70. Adequacy of Representation: Plaintiff is a more than adequate representative of the Class in that Plaintiff's PII was compromised and has suffered damages. In addition:

- a. Plaintiff is committed to the vigorous prosecution of this action on behalf of herself and all others similarly situated and has retained competent counsel experienced in the prosecution of class actions and, in particular, class actions regarding data breaches;
- b. There is no conflict of interest between Plaintiff and the unnamed members of the Class or Subclass;
- c. Plaintiff anticipates no difficulty in the management of this litigation as a class action; and
- d. Plaintiff's legal counsel have the financial and legal resources to meet the substantial costs and legal issues associated with this type of litigation.

71. Plaintiff knows of no difficulty to be encountered in the maintenance of this action that would preclude its maintenance as a class action.

72. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all of Plaintiff's and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

73. Lakeland has acted or refused to act on grounds generally applicable to the Class and Subclass, thereby making appropriate corresponding declaratory relief with respect to the Class and Subclass as a whole. Lakeland's actions and inactions challenged herein apply to and affect Class Members uniformly and hinges on its conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

74. Superiority of Class Action. The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain class members, who could not individually afford to litigate a complex claim against a large organization like Defendant. Further, even for those class members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

75. The nature of this action and the nature of laws available to Plaintiff and the Class make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and the Class for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

76. The litigation of the claims brought herein is manageable. Lakeland's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

77. Adequate notice can be given to Class Members directly using information maintained in Lakeland's records.

78. Unless a Class-wide injunction is issued, Lakeland may continue in its failure to properly secure the PII of Class Members, may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and may continue to act unlawfully as set forth in this Complaint.

79. All conditions precedent to bringing this action have been satisfied and/or waived.

FIRST CAUSE OF ACTION
Breach of Contract
(On Behalf of Plaintiff and the Classes)

80. Plaintiff and the class re-allege and incorporate by reference each and every preceding paragraph of this Complaint.

81. Plaintiff and Class members entered into a valid and enforceable contract through which they paid money to Lakeland in exchange for educational and other services. That contract included promises by Defendant to secure, safeguard, and not disclose Plaintiffs' and Class Members' Private Information.

82. Lakeland's Privacy Policy memorialized the rights and obligations of Lakeland and its students and employees. This document was provided to Plaintiffs and Class Members became part of the agreement for services.

83. In its Privacy Policy, Lakeland commits to protecting the privacy and security of the PII belonging to its students, including Plaintiff and Class members, and promises to never share this Private Information except under certain limited circumstances.

84. Plaintiff and Class members fully performed their obligations under their contracts with Lakeland.

85. However, Lakeland did not secure, safeguard, and/or keep private Plaintiff's and Class members' PII and therefore Lakeland breached its contracts.

86. Lakeland allowed third parties to access, copy, and/or exfiltrate PII without permission. Therefore, Lakeland breached the Privacy Policy with Plaintiff and Class members.

87. Lakeland's failure to satisfy its confidentiality and privacy obligations resulted in Lakeland providing services to Plaintiff and Class members that were of a diminished value.

88. As a result, Plaintiff and Class members have been harmed, damaged, and/or injured as described herein, including in Defendant's failure to fully perform its part of the bargain with Plaintiff and Class members.

89. As a direct and proximate result of Lakeland's conduct, Plaintiff and Class members suffered and will continue to suffer damages.

90. In addition to monetary relief, Plaintiff and Class members are also entitled to injunctive relief requiring Lakeland to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class members.

SECOND CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Classes)

91. Plaintiff and the class re-allege and incorporate by reference each and every preceding paragraph of this Complaint.

92. This Count is pleaded in the alternative to Count I above.

93. When Plaintiff and members of the Class provided their PII to Lakeland, Plaintiff and members of the Class entered into implied contracts with Lakeland pursuant to which Lakeland agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class members that their data had been breached and compromised.

94. Defendant's implied promises to Plaintiff and Class members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to PII also protect the confidentiality of that data; (2) taking steps to ensure that the PII that is placed in the control of its employees is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees and/or agents; (4) designing and implementing

appropriate retention policies to protect the PII against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; and (7) taking other steps to protect against foreseeable data breaches.

95. Defendant required Plaintiff and Class members to provide and entrust their PII and financial information as a condition of enrolling and obtaining Defendant's services.

96. Plaintiff and Class members would not have provided and entrusted their PII and financial information to Lakeland in the absence of the implied contract between them and Lakeland.

97. Plaintiff and members of the Class fully performed their obligations under the implied contracts with Lakeland.

98. Lakeland breached the implied contracts it made with Plaintiff and Class members by failing to safeguard and protect the personal information of Plaintiff and members of the Class and by failing to provide timely and accurate notice to them that their personal information was compromised in and as a result of the Data Breach.

99. The losses and damages sustained by Plaintiff and Class members as described herein were the direct and proximate result of Lakeland's breaches of the implied contracts between Lakeland and Plaintiff and members of the Class.

THIRD CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Classes)

100. Plaintiff and the Class restate and reallege all proceeding allegations above as if fully set forth herein.

101. This count is brought in the alternative to Plaintiff's breach of contract counts. If the claims for breach of contract are ultimately successful, this count will be dismissed.

102. Plaintiff and Class members conferred a benefit on Lakeland by way of customers' paying Lakeland to maintain Plaintiff and Class members' personal information.

103. The monies paid to Lakeland were supposed to be used by Lakeland, in part, to pay for the administrative and other costs of providing reasonable data security and protection to Plaintiff and Class members.

104. Lakeland failed to provide reasonable security, safeguards, and protections to the personal information of Plaintiff and Class members, and as a result Lakeland was overpaid.

105. Under principles of equity and good conscience, Lakeland should not be permitted to retain the money because Lakeland failed to provide adequate safeguards and security measures to protect Plaintiff's and Class members' personal information that they paid for but did not receive.

106. Lakeland wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class members.

107. Lakeland's enrichment at the expense of Plaintiff and Class members is and was unjust.

108. As a direct and proximate result of Lakeland's conduct, Plaintiff and Class members have suffered and/or will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity

theft; (vi) the continued risk to their PII, which remains in Lakeland's possession and is subject to further unauthorized disclosures so long as Lakeland fails to undertake appropriate and adequate measures to protect PII in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

109. Plaintiff and Class members are entitled to full refunds, restitution, and/or damages from Lakeland and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Lakeland from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class members may seek restitution or compensation.

110. As a result of Lakeland's wrongful conduct, as alleged above, Plaintiff and the Class are entitled to restitution and disgorgement of profits, benefits, and other compensation obtained by Lakeland, plus attorneys' fees, costs, and interest thereon.

FOURTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Classes)

111. Plaintiff and the Class restate and reallege all proceeding allegations above as if fully set forth herein.

112. This cause of action is brought under 28 U.S.C. § 2201. This Court is authorized to declare rights, status, and other legal relations, and such declarations shall have the force and effect of a final judgment or decree. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious as described in this Complaint.

113. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII. Plaintiff alleges that Defendant's data security measures remain inadequate, contrary to its assertion that it has confirmed the security of its network and its systems.

114. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of PII and remains at imminent risk that further compromises will occur in the future.

115. This Court should enter a judgment declaring, among other things, the following:

- a. Defendant owes a legal duty to secure PII and to timely notify those affected of the Data Breach; and
- b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure PII.

116. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect PII.

117. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach. The risk of another such breach is real, immediate, and substantial. If another breach at Lakeland occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

118. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Lakeland if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Lakeland of complying with an injunction by employing reasonable prospective data security measures and communicating

those measures to the Class is relatively minimal, and it has a pre-existing legal obligation to employ such measures.

119. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Lakeland, thus eliminating the additional injuries that would result to Plaintiff and to those whose PII would be further compromised.

120. Plaintiff and the Class, therefore, seek a declaration (1) that Lakeland's existing security measures do not comply with their contractual obligations and duties of care to provide adequate security, and (2) that to comply with their obligations and duties of care, Lakeland must implement and maintain reasonable security measures, including, but not limited to, the following:

- a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;
- c. Ordering that Defendant audit, test, and train their security personnel regarding any new or modified procedures;
- d. Ordering that Defendant segment PII data by, among other things, creating firewalls and access controls so that if one area of Defendant's system is compromised, hackers cannot gain access to other portions of Defendant's systems;
- e. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner all data not necessary for its provisions of services;
- f. Ordering that Defendant conduct regular computer system scanning and security checks;
- g. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to

identify and contain a breach when it occurs and what to do in response to a breach; and

- h. Ordering Defendant to meaningfully educate employees and members about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all other similarly situated, prays for relief as follows:

- A. For an order certifying the Class and Subclass and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;
- B. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;
- C. For compensatory, statutory, treble, and/or punitive damages in amounts to be determined by the trier of fact;
- D. For an order of restitution and all other forms of equitable monetary relief;
- E. Declaratory and injunctive relief as described herein;
- F. Awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;
- G. Awarding pre- and post-judgment interest on any amounts awarded; and
- H. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Date: October 2, 2023

Respectfully submitted,

/s/Christopher Wiest
Christopher Wiest (Ohio 0077931)
25 Town Center Blvd., Suite 104
Crestview, KY 41017
Tel: (513) 257-1895
Fax: (859) 495-0803

chris@cwestlaw.com

Kenneth Grunfeld*
KOPELOWITZ OSTROW, P.A.
65 Overhill Road
Bala Cynwyd, Pennsylvania 19004
Main: 954-525-4100
grunfeld@kolawyers.com

Attorneys for Plaintiff and Proposed Class

**Pro hac vice or applications for admission
to be filed*